Minutes of the meeting of the Audit and Compliance Committee of the Board of Directors of the Cook County Health and Hospitals System held Thursday, November 15, 2018 at the hour of 9:00 A.M. at 1950 W. Polk Street, in Conference Room 5301, Chicago, Illinois.

I. Attendance/Call to Order

Acting Chair Hammock called the meeting to order.

Present: Acting Chair M. Hill Hammock (Substitute Member) and Directors Ada Mary Gugenheim and Layla P. Suleiman Gonzalez, PhD, JD (3)

Absent: Chair Hon. Jerry Butler and Director Robert G. Reiter, Jr. (2)

Additional attendees and/or presenters were:

Cathy Bodnar – Chief Corporate Compliance and Privacy Officer
Debra Carey – Deputy Chief Executive Officer, Operations
Douglas Elwell – Deputy Chief Executive Officer, Finance and Strategy
Donna Hart – Chief Information Officer
Jeff McCutchan –General Counsel
Deborah Santana – Secretary to the Board
Tom Schroeder – Director of Internal Audit
Dean Sorensen – Information Security Officer

II. Public Speakers

Acting Chair Hammock asked the Secretary to call upon the registered public speakers.

The Secretary responded that there were none present.

III. Report from Chief Corporate Compliance and Privacy Officer (Attachment #1)

Cathy Bodnar, Chief Corporate Compliance and Privacy Officer, provided an overview of the information contained in the Report. Dean Sorensen, Information Security Officer, reviewed the information regarding security intelligence and controls. The Committee reviewed and discussed the information.

The report included information on the following subjects:

- Review Privacy and Security Rules
- Recognize the National Landscape
- Discuss Current Internal Activity
- View Cook County Health Measures for Compliance – Proactive and Reactive

During the review of the information regarding security intelligence and controls, the Committee discussed the subject of securing the health information exchange between CCHHS providers and providers from outside organizations who share data on a patient. Mr. Sorensen stated that those exchanges can be secure, but the organizations have to be on the same page on how to do it. Donna Hart, Chief Information Officer, provided additional information regarding MHN Connect, which is a mechanism that allows this organization to receive and share information in a secure fashion on patients with other organizations who are part of that network.

IV. Action Items

A. Minutes of the Audit and Compliance Committee Meeting, September 20, 2018

Director Suleiman Gonzalez, seconded by Director Gugenheim, moved to accept the minutes of the Audit and Compliance Committee Meeting of September 20, 2018. THE MOTION CARRIED UNANIMOUSLY.

B. Any items listed under Sections IV and V

V. Closed Meeting Items

A. Report from Director of Internal Audit
B. Discussion of Personnel Matters

Director Gugenheim, seconded by Director Suleiman Gonzalez, moved to recess the open meeting and convene into a closed meeting, pursuant to the following exceptions to the Illinois Open Meetings Act: 5 ILCS 120/2(c)(**1**), regarding "the appointment, employment, compensation, discipline, performance, or dismissal of specific employees of the public body or legal counsel for the public body, including hearing testimony on a complaint lodged against an employee of the public body or against legal counsel for the public body to determine its validity," and 5 ILCS 120/2(c)(**29**), regarding "meetings between internal or external auditors and governmental audit committees, finance committees, and their equivalents, when the discussion involves internal control weaknesses, identification of potential fraud risk areas, known or suspected frauds, and fraud interviews conducted in accordance with generally accepted auditing standards of the United States of America." THE MOTION CARRIED UNANIMOUSLY

Acting Chair Hammock declared that the closed meeting was adjourned. The Committee reconvened into the open meeting.

VI. Adjourn

As the agenda was exhausted, Acting Chair Hammock declared the meeting ADJOURNED.

Respectfully submitted,
Audit and Compliance Committee of the Board of Directors of the Cook County Health and Hospitals System

XXXXXXXXXXXXXXXXXXXXXX
M. Hill Hammock, Acting Chair

Attest:

XXXXXXXXXXXXXXXXXXXXXX
Deborah Santana, Secretary

Requests/Follow-up:

There were no requests for follow-up at this meeting.

ATTACHMENT #1

AUDIT & COMPLIANCE COMMITTEE OF THE BOARD OF DIRECTORS

Corporate Compliance Report

November 15, 2018

COOK COUNTY HEALTH & HOSPITALS SYSTEM
CCHHS

Meeting Objectives

- Review Privacy & Security Rules
- Recognize the National Landscape
- Discuss Current Internal Activity
- View CCH Measures for Compliance
  - Proactive
  - Reactive

The "Alphabet Soup" of Privacy

- The Health Insurance Portability and Accountability Act
  - 2003 – HIPAA Privacy Rule
  - 2005 – HIPAA Security Rule
- Patient/member privacy rights related to health data
- Key Terms:
  Protected Health Information (PHI) and
  Electronic Protected Health Information (ePHI)
- CCH has a responsibility to safeguard PHI and ePHI

REUTERS

TECHNOLOGY NEWS OCTOBER 19, 2018 / 4:56 PM / 6 DAYS AGO

U.S. CMS says 75,000 individuals' files accessed in data breach

(Reuters) - The U.S. Centers for Medicare & Medicaid Services (CMS) said on Friday it was responding to a data breach that exposed the files of about 75,000 individuals.

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

March 13, 2018
By Elizabeth Snell

A New York surgery center reported a potential data breach stemming from a server being accessed by an unauthorized user.

TULSA WORLD

Data breach at OSU Center for Health Sciences may have exposed Medicaid patient information

From Staff Reports Jan 5, 2018

Nearly 280,000 Medicaid patient records breached in Oklahoma State University Center for Health Sciences.

Modern Healthcare
The leader in healthcare business news, research & data

Anthem to pay $16M in record data breach settlement

By Erica Teichert | October 16, 2018

Anthem has agreed to pay the federal government $16 million in a settlement over its 2015 data breach that hit nearly 79 million people, HHS said Monday.

The agreement is by far the largest settlement reached by HHS' Office for Civil Rights for a Health Insurance Portability and Accountability Act breach. Hackers stole the names, birth dates, Social Security numbers, home addresses and other personal information in the 2015 cyberattack.

As part of the settlement, Anthem agreed to a corrective action plan where it will conduct a risk analysis and fix any deficiencies. HHS will oversee Anthem's work.

Des Moines Register
PART OF THE USA TODAY NETWORK

UnityPoint warns 1.4 million patients their information might have been breached by email hackers

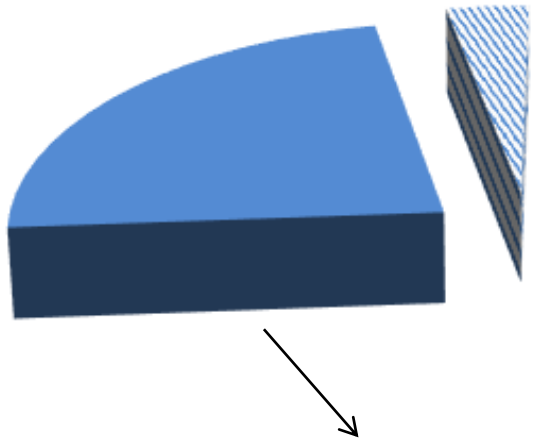
Tony Leys, Des Moines Register Published 3:42 p.m. CT July 30, 2018 | Updated 4:22 p.m. CT July 30, 2018

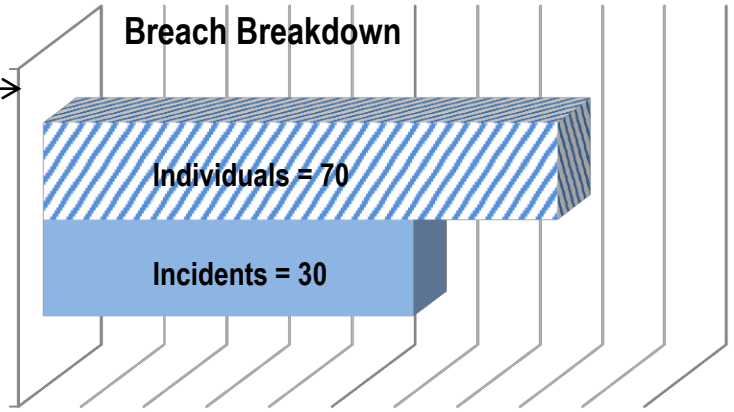
Privacy Allegations Received by Compliance

F-YTD 238 Issues Attributed to HIPAA

26% of the Total Issues Received F-YTD

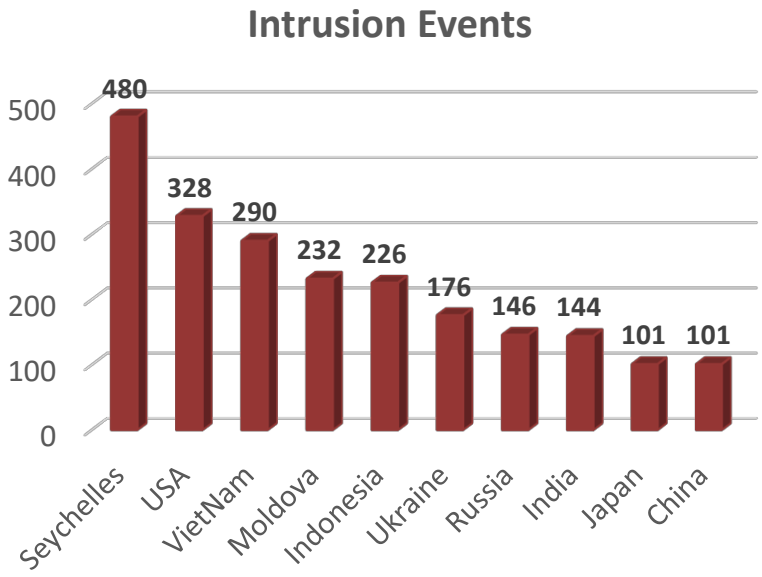
Of the 238 Privacy allegations received, 13% or 30 incidents were validated privacy breaches



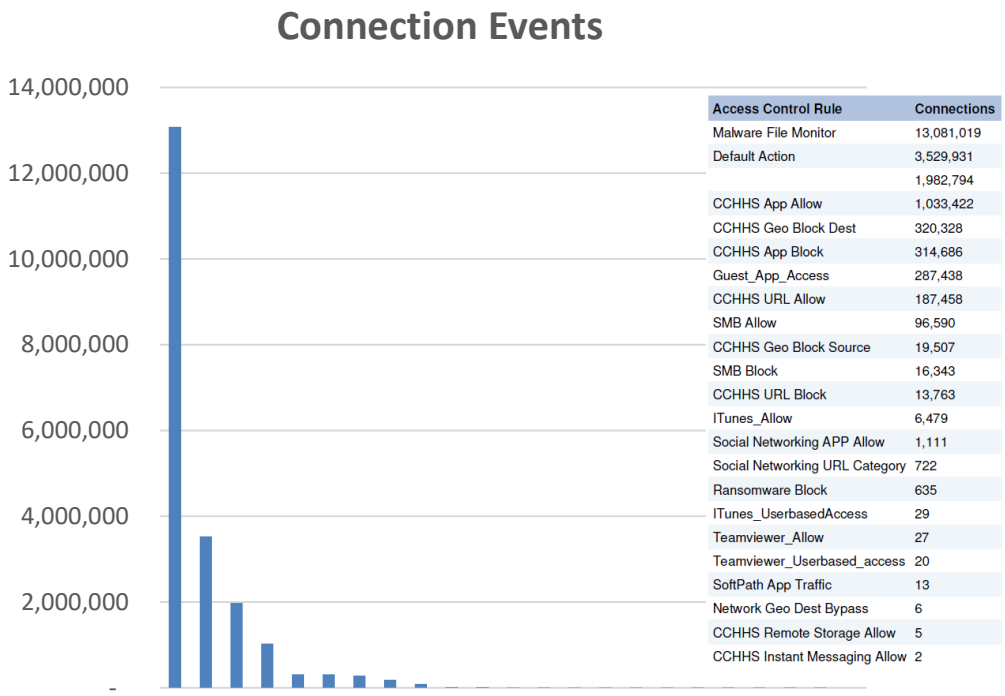


Other Privacy matters = 87% (Determination of no breach and guidance requests, e.g. Contract and Business Associate Agreement, data sharing, subpoena requests)

Security Intelligence



Sample Reports Received Monthly



Access Control Rule	Connections
Malware File Monitor	13,081,019
Default Action	3,529,931
	1,982,794
CCHHS App Allow	1,033,422
CCHHS Geo Block Dest	320,328
CCHHS App Block	314,686
Guest_App_Access	287,438
CCHHS URL Allow	187,458
SMB Allow	96,590
CCHHS Geo Block Source	19,507
SMB Block	16,343
CCHHS URL Block	13,763
ITunes_Allow	6,479
Social Networking APP Allow	1,111
Social Networking URL Category	722
Ransomware Block	635
ITunes_UserbasedAccess	29
Teamviewer_Allow	27
Teamviewer_Userbased_access	20
SoftPath App Traffic	13
Network Geo Dest Bypass	6
CCHHS Remote Storage Allow	5
CCHHS Instant Messaging Allow	2

CCH Proactive & Reactive Measures

Security Tools

- Intruder Prevention (Cisco Firepower)
- MS Office 365 (Recent Optimizations)
- Infoblox Secure DNS (How it helps with Phishing Attacks)
- Cerner 724 Read-Only upgrade to 724 Access Downtime Viewer (Business Continuity Plan/Disaster Recovery)
- Cerner Instant Access (Security and Authentication)

Additional Security Controls

- Updated privacy & security training
- Adapted policies to evolving environment including
  - Mobile Device Management
    (also implementing controls)
- Developed vendor questionnaire

Future Initiatives

- Optimizing medical device management
- Developing an anti-phishing program
- Enhancing asset control through IT Service Management (ITSM)
- Requiring multi-factor-authorization (remote access)